
# Secure Personal Identification Systems:

## Policy, Process and Technology Choices for a Privacy-Sensitive Solution

*A Smart Card Alliance White Paper*

*February 2002*

**Smart Card Alliance**
191 Clarksville Road
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 212-571-0100

## Overview

Recent events have heightened interest in implementing more secure personal identification (ID) systems to improve confidence in verifying the identity of individuals seeking access to physical or virtual locations. A secure personal ID system must be designed to address government and business policy issues and individual privacy concerns. The ID system must be secure, provide fast and effective verification of an individual's identity, and protect the privacy of the individual's identity information.

Smart card technology is the best platform for a secure personal ID system. A smart card based system delivers a proven, cost-effective solution that meets government and business requirements for secure and accurate identity verification, while also meeting the individual's need for information privacy. Coupled with a secure, privacy-sensitive information technology (IT) architecture and policy framework, a smart card based secure personal ID system can provide accurate personal identification, protect an individual's personal information, and best address the policy and legal requirements that are currently being debated.

This paper describes policy, process and technology issues that need to be considered in implementing a privacy-sensitive secure personal ID system. The different ID technologies that are available are compared, and the role that smart cards can play in implementing trusted personal credentials is presented.

## Secure Personal ID Applications

Individuals are required currently to confirm their identity for many purposes – from verifying identity and eligibility within a healthcare system, to accessing a secure network, to proving identity for travel. A heightened interest in physical security, coupled with increasing requirements to provide secure network access, have led many government agencies, industry groups and businesses to intensify their efforts to define solutions that can improve the security of personal identification systems. Solution requirements may include providing secure identification for physical access, for logical access (e.g., for secure sign-on to networks) and for authenticated application, data or service access within a system. A few prominent examples of current initiatives are summarized below.

**Voluntary travel identification card**

A number of groups in the U.S. are advocating the creation of a voluntary travel identification card to verify passenger identity. The Air Transport Association and other airline officials are supporting the issuance of these cards, which would embed passenger biometric templates and other identifying information. Individuals who apply for and hold this card would be able to avoid long lines at airport security checkpoints.

**Immigration**

There is heightened interest in providing secure identification cards for foreign visitors to reduce the number of forged and counterfeited cards and to improve immigration control at borders. Advocates for these cards envision them including personal biometric data and cardholders having the biometric scanned and matched to prove identity. Both the U.S. and Canada have introduced legislation or announced plans for an improved immigration identification system. The *Visa Entry Reform Act of 2001* was recently introduced by Senators Dianne Feinstein (D-Calif.) and John Kyl (R-Ariz.). Among other process and program reforms, the act would create a centralized database of visitors in the U.S. and develop a new biometric visa card that the INS and State Department would issue to foreign nationals. In Canada, Elinor Caplan, Minister of Citizenship and Immigration, announced a new anti-terrorism plan that would accelerate the issuance of a credit card-sized permanent resident card, compatible with the U.S. Permanent Resident Card, to reduce fraud, improve the integrity of the immigration system, and allow easier travel for legal immigrants.

**Driver's license**

The American Association of Motor Vehicle Administrators (AAMVA) has created a Special Task Force on Identification Security. This task force is working on a plan to strengthen the security of the driver's license, which has, according to the group, "become the 'de facto' national identification card used by law enforcement, retailers, banks and other establishments requiring proof of identification." By providing a uniform approach and set of standards, states would be able to issue a more secure driver's license that could be used, in many instances, as a common secure personal ID for individuals.

**Employee identification**

Virtually every government and company employee carries some form of employee identification. Many employers are now improving their identification systems to expand functionality from simple physical identification to identification for a broad range of applications including: physical and logical access; submission of claims for medical or other employee benefits; control and management of corporate assets; and replacement of paper-based processes with online forms. Examples of smart card based employee ID initiatives follow.

- The U.S. Department of Defense (DoD) has initiated a program to issue a smart card based "common access card" to all military and civilian employees and contractors. DoD employees will use these cards to digitally sign and encrypt documents and to have secure access to buildings and networks.
- The U.S. Department of State is in the process of implementing a new automated access control system for employees and visitors using a smart ID card.
- The Federal Deposit Insurance Corporation (FDIC) has a smart card based public key infrastructure (PKI) system in place for remote access to central databases by bank auditors.
- Royal Dutch/Shell Group has announced the issuance of over 85,000 smart cards to employees worldwide to provide secure physical and network access, as well as corporate ID, on one card.

While each of the above initiatives has specific distinct requirements for a secure personal ID system, they are all trying to solve a common problem: providing an individual with a recognized credential that is the result of a trusted process to confirm identity and that is effective and efficient at proving identity either in person or over a network.

It is likely that multiple organizations will issue improved secure personal ID cards to address heightened concerns about national security. The focus of these efforts will be on implementing a system that automates the identity verification process (i.e., uses machine-assisted authentication). Smart card technology, along with other complementary approaches, is the solution foundation for many identification-related applications.

## Policy and Secure Personal Identification Systems

The implementation of secure personal identification systems depends on a wide range of governmental or corporate policy issues. Currently, many identification systems rely on staff to visually inspect low security paper or photo IDs presented for identification (e.g., passports, visas, drivers licenses). Individuals are accustomed to using these traditional identification technologies and processes in their daily life. However, most photo IDs, including driver's licenses, do not leverage the latest in personal identification or security technologies and are relatively easy to counterfeit and use fraudulently. Yet privacy and individual rights advocacy groups are voicing concerns that proposals to issue ID cards based on newer technologies could tread upon civil liberties. For example:

- How invasive will any new biometric identification processes become – e.g. are retinal or iris scans too invasive?
- How secure is personal information stored on or accessed by an identification card? Who has access to this information?
- Would a new identification card become mandatory, or would it work side by side with traditional ID systems for those citizens who prefer not to use new identification technologies?

Consumer privacy and civil liberties groups also fear that the linkage of government and corporate databases could lead to personal information being accessed without an individual's knowledge. Clearly policy makers must not ignore these concerns. Any identification system is open to abuse unless the right policies, legislation, processes and technologies are in place to protect the individual.

Figure 1 summarizes the policy decisions, system requirements and solution features that may be considered in a secure personal identification system deployment. Policy issues can range from the establishment of agreed upon standards among participating countries to the degree of authentication needed for individuals.

Card management policies and processes also need to be designed and implemented to support secure personal ID applications. A card issuance process must accurately verify the identity of the recipient at the beginning of the process. Individual identity information must be acquired and securely stored. Once cards are issued, identity information must be securely maintained and synchronized among applications and with new updated information. The governance and management of the secure personal ID card system must take into account privacy issues and the infrastructure cost of the system deployment.

Smart card based identification solutions are able to meet the requirements of a wide range of policy and legal mandates. Smart cards are a powerful tool for improving the security of any personal identification system AND protecting an individual's privacy rights. A smart card based ID system can support a machine-assisted identification process, limiting the potential bias or judgment errors in identifying people. Coupled with a secure, privacy-sensitive IT architecture, a smart card based personal ID system can provide accurate personal identification, protect an individual's personal information, and address the policy and legal requirements that are currently being debated.

**Figure 1: Policy Issues Considered in a Secure Personal ID System Implementation**

| Policy | Requirements | Solution |
|---|---|---|
| Voluntary vs. Mandatory | • Card is an alternative form factor to traditional ID forms, or<br>• Card becomes a mandatory ID requirement for all citizens | • Solutions are designed to co-exist with traditional ID processes, or<br>• Solutions are designed to replace the existing photo ID process. |
| Governance | • Requirements will specify responsibilities and roles for authorities involved in oversight, administration and enforcement of an ID program. | • Build solutions that can work with fragmented databases.<br>• Design the IT architecture to ensure that cross-organization systems are integrated, communicate in near real time, and provide secure data storage. |
| Privacy | • Specify the amount of information stored for each individual.<br>• Specify where this information should be stored and how it is protected from unauthorized access.<br>• Specify who is entitled to have access to the identification information. | • Individual information can be stored in a secure centralized database, locally on a card or in both central and local locations.<br>• Build a solution that allows the individual to control who has access to the identification information. |
| Degree of Authentication | • Issuing authorities or governments will specify the degree of authentication, based on the level of risk.<br>• The general public will voice their opinions on the acceptability of the level of authentication and type of biometric scan. | • Design a solution that incorporates:<br>(1) Something you have: Smart card or another type of ID.<br>(2) Something you know: PIN or passcode.<br>(3) Something you are: Biometric information (e.g., iris, hand geometry, fingerprint, voice print, facial scan). |
| Standards | • Specify which countries the solution should be compatible with and which standards it should support | • Build technology solutions based on industry standards to allow the widest compatibility and availability of components. |
| Profiling | • Specify the amount and type of information applied for risk profiling (e.g., age, gender, ethnicity, country of origin, traveler profile, criminal records, employment history) | • Design a technology solution that can interface with any number of databases.<br>• Build risk profile algorithms based upon government specifications and needs and that can evolve and be upgraded over time. |
| Mechanisms for ID Issuance | • Specify the allowable means for proving an identity is valid prior to ID issuance. | • Define system-level processes and procedures to implement the desired level of risk management. |

## ID Card Technology Alternatives

A number of commercially available technologies can be considered in the design of a personal identification system. This section defines the types of ID card technologies that are currently available and discusses their relative advantages and disadvantages in the implementation of a privacy-sensitive system.

**Plastic cards**. Simple plastic cards with printed visual identification information (e.g., individual name, address, photo) are used in numerous applications where information is visually verified when the card is presented for identification.

**Bar codes**. Bar codes can store personal information and can be printed on plastic cards. Linear bar codes are used to store simple alphanumeric data (e.g., in retail applications). Two-dimensional bar codes can now store significantly more data in a small amount of space. Data is translated into a bar code and embedded on the card during the printing process. The card is then scanned at the point of interaction.

**Magnetic stripe cards**. Magnetic stripes have been used on cards since the 1970s for a wide range of applications – from financial credit cards to transit cards to driver's licenses. Identification information is written to the magnetic media during the personalization process and then read by swipe or insertion readers at the point of interaction. A new magnetic stripe standard for cards will provide more memory capacity than available with previous cards.

**Optical stripe cards**. Optical stripe cards use a technology that is similar to the one used to read and write CDs. Cards with an optical stripe use Write Once Read Many (WORM) recording technology, allowing data to be read and added, but not deleted or erased. Optical stripe cards have an extremely high (multiple megabytes), non-volatile memory capacity and are used in identification, healthcare, logistics management and other applications requiring storage of a large amount of data.

**Smart cards**. A smart card includes an embedded computer chip that can be either a microprocessor with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microprocessor, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are used worldwide in financial, telecommunications, transit, healthcare, secure identification and other applications.

The use of **biometric technology** is widely believed to be essential in any secure personal ID system design. Biometrics can be used with the card technologies discussed above (e.g. smart cards), where biometric information is stored on the card and then verified with the received biometric at the point of interaction. By securely recording and then checking an individual's unique biometric information (e.g., fingerprints, hand geometry, retinal or iris patterns, facial patterns or voiceprints), the system can validate the individual's identity. The verification process may be done by the smart card or by a biometric-specific reader. Alternatively, a central database of biometric information can be used, with an online screening device.

## Technology Evaluation

When evaluating alternative technologies used in a secure personal identification system design, there are several key questions that should be considered.

***1. What types of information need to be stored on the personal ID card?***

A typical secure personal ID card will include text information about the individual (name, address, ID number), compressed photo image, one or more biometrics, and security functions (such as digital signatures and public/private keys). Figure 2 shows the memory required for a variety of biometric templates. Both the smart card and optical stripe card have larger memory sizes, making them more attractive for biometrics-based systems. Smart card memory will hold data, applications and the card operating system.

**Figure 2: Biometric Template Size**
*Source: Frost & Sullivan*

| Biometric | Bytes Required |
|---|---|
| Finger-scan | 300-1200 |
| Finger geometry | 14 |
| Hand geometry | 9 |
| Iris recognition | 512 |
| Voice verification | 1500 |
| Face recognition | 500-1000 |
| Signature verification | 500-1000 |
| Retina recognition | 96 |

***2. What level of security is required to implement the desired risk management profile?***

Identification systems based on paper documents have been subject to widespread fraud and identity theft. An ID card and ID card system must be secure – i.e., resistant to fraud, ID theft, and counterfeiting. A secure personal ID card must be sufficiently difficult to produce, be protected by security design features so that it is extremely difficult to counterfeit, and be able to invalidate itself when tampered with. Card security functions must include features to prevent unauthorized access to and use of any card data (for example, using encryption to enhance the card's basic security level). A microprocessor-based smart card has the unique ability to use active security methods that require on-card computations or interactions with the reader. Because of this, smart cards can provide a higher degree of security and individual privacy than other technologies.

***3. What is the potential future use of the personal ID card system and how will the system be upgraded to handle new requirements and features?***

A key requirement for any identification system is the ability for the system to be upgraded without needing large investments in new infrastructure. Upgradability is critical since new requirements may drive new system functionality or there may be a need to modify the system without replacing the individual identity cards if a security scheme is compromised. Smart cards allow the most flexibility for updates to the card data and for secure management of multiple applications (e.g., allowing new applications to be added incrementally over time).

### *4. What standards-based technologies are available?*

Identification systems will be implemented by many business and governmental organizations, using different and often proprietary technologies. This diversity of technologies makes it more difficult to detect counterfeiting, limits the use and expandability of the cards, and often locks the issuer into a limited number of product vendors. The ideal system would define an open architecture for cards and other equipment, using a common card specification standard. The standard would enable cards to be used for multiple purposes, if desired, and allow organizations to purchase cards from a variety of vendors, keeping costs lower. All of the card technologies discussed in this section are based, at some level, on lSO, ANSI or other industry standards. The degree of standardization and number of vendor products available, however, varies by technology. Appropriate standards should be considered in a secure personal identification system design to ensure that multiple vendors are able to supply both cards and readers.

### *5. How will card readers be used in the identification process? What are projected transaction volumes and required transaction speeds?*

To read card information, cards can be swiped (magnetic stripe), scanned (bar code), sensed (contactless smart card) or inserted into a reader (read/write magnetic stripe, optical or smart card). Both read/write magnetic stripe and optical card readers require moving parts during the transaction process, resulting in higher reader acquisition and maintenance costs. Smart card and read-only magnetic stripe readers have relatively low costs (<$20) when purchased in volume and are robust for high volume applications. The overall transaction time will include the card reading/writing time and the time required for any biometric check. In high volume applications, the ability to have the reader interact with the ID card without making direct physical contact (e.g., with a contactless smart card) may be critical to achieving the desired throughput.

### *6. What needs to be considered in determining the overall cost of the secure personal identification system?*

The physical ID card contributes a small fraction of the total cost in the overall deployment of a secure identification system. The total system cost includes ID card design, issuance and management costs, card reader cost, biometric reader cost (to read the individual's physical biometric, if desired), and other supporting infrastructure costs. Costs also include the redesign of identity verification processes, and personnel retraining and staffing. The design of any secure personal ID system must balance the total cost (initial and on-going) with the desired risk management profile. For systems requiring a high degree of security, smart cards provide a proven, cost-effective solution, balancing initial cost with the highest security architecture and the flexibility to more easily modify and upgrade the system over time.

Figure 3 summarizes important features of card and card reader technologies that are typically considered when making a technology selection. Additional detailed information about this matrix can be found in the Frequently Asked Questions document at www.smartcardalliance.org.

**Figure 3: Comparison of Alternative ID Technologies**

| | Card Features and Characteristics | | | | | Reader Features | |
|---|---|---|---|---|---|---|---|
| **Card Type** | **Security [1]** | **Typical Memory Size [2]** | **Multi-Application Support** | **Standards** | **Upgrad-ability [3]** | **Reader Technology** | **Reader Portability** |
| **Smart Card** | ● | ● | ● | ● | ● | Solid state | ● |
| **Plastic** | ○ | ○ | None | ● | None | N/A | N/A |
| **Magnetic Stripe** | ◐ | ○ | ○ | ● | ◐ | Solid state, moving parts | ● |
| **2D Barcode** | ◐ | ◐ | ○ | ● | ◐ | Solid state optics | ● |
| **Optical** | ◐ | ● | ● | ● | ◐ | Solid state, moving parts | ○ |

**Relative Position:** Strong ● Medium ◐ Weak ○

**Notes:**

(1) The rating for the security of the ID card evaluated in this matrix takes into account the ability for the ID card to be used on a network, provide active security functions and help with e-government services.

(2) The maximum memory size required by most ID applications is less than 20 Kbytes. In this matrix, technologies with less than 2 Kbytes get the weakest position and those with more than 10 Kbytes get the strongest position.

(3) Upgradability of an ID card as part of a system takes into account the ability of the card itself to store and enforce new security features, program functions, algorithms or keys, without changing reader infrastructure.

While the discussion above focuses on a secure personal identification card that would use only one of the technologies described, cards can be manufactured with a combination of technologies. For example, the DoD common access card mentioned earlier is a combination magnetic stripe, bar code, photo ID and smart card. By including multiple technologies, the DoD was able to use the card with existing legacy systems, simplifying the migration process. Another example is the Italian National ID card that uses an optical stripe for authentication, positive ID, and backup, along with a smart card chip for e-government services. There are also alternative form factors (e.g. USB tokens or PCMCIA cards) which are not discussed in this paper and that could be considered. These form factors are more typically considered when there is no need for a photo on the ID card or when the identification token is being used for secure network access.

## The Role of Smart Cards in Secure Personal ID Systems

Widely acknowledged as the most secure and reliable form of electronic identification, smart cards can act as the individual's secure personal identification card and allow access to information and services in both online and offline system designs. With the ability to store, protect and modify information written to the card's microchip, smart cards offer unmatched flexibility and options for information sharing and transfer, while providing the unique ability to incorporate privacy-sensitive features. The card's dynamic ability to communicate with information systems speeds traditionally lengthy identification processes, while streamlining operations and reducing costs. Moreover, the smart card's ability to host multiple applications enables the consolidation of multiple services on one card, promoting additional cost savings and efficiency.

Smart cards provide an optimal technology platform for a secure personal ID system that can meet government and business requirements for secure and accurate identification verification while also meeting individuals' needs for information privacy. This section summarizes some of the unique features that smart cards bring to a secure personal ID system design.

**Physical and Digital Identity**. Smart cards provide the unique capability to easily combine identification and authentication in both the physical and digital worlds. This can generate significant savings as the smart card based personal identification card could not only be used to allow physical access to services, but also allow individuals to file taxes, access social security information and request official papers (e.g., birth certificate) online.

- **Secure physical identification** is provided by visual printed information and security printing technologies on the smart card.
- **Physical authentication** can be accomplished either by using a unique PIN for the card or by storing the card owner's biometric information (e.g., fingerprint) on the chip. Both of these approaches will enable the smart card to operate only after the card user has successfully verified ownership of the card by matching data stored in the chip.
- **Digital identification** is provided by the personal information stored in the chip (e.g., name, age, address, social security number) related to the identification, or "role," the individual wants to prove in a given transaction. Different transactions will require different information to be provided – for example, the individual's age to buy cigarettes, the social security number to file documents with the IRS, a traveler profile to quickly verify identity at airports, or the driver's license number for an encounter with a police officer.
- **Digital authentication** is provided by cryptographic keys and digital certificates stored in the chip, securing the personal information stored in the card and giving proof of the information authenticity, as verified by the certifying authority.

**Authenticated and Authorized Information Access**. Most of the physical and digital identification features can be achieved by other ID technologies, provided that the information is simply verified by the receiving party. Along with the strong information protection and security that is inherent to smart card technology, the smart card's ability to process information and react to its environment presents a unique advantage that other technologies cannot offer. All of the individual's personal information does not need to be revealed – every time – to prove identity. The information required for identification can depend on the given "role" for the individual at a given point in time. For example, when cigarettes are being purchased, only age is required. The fact that the individual can or can't drive and the individual's address are irrelevant.

**A smart card is an active token**. A smart card is able to give the information required, and ONLY this information when required. The card's unique ability to verify the authority of the information requestor allows it to be the best guardian of the owner's personal information. For example, to a police officer, a smart card will present information related to the motor vehicle authority (and this may depend on the state issuing the license). By allowing authorized, authenticated access only to the information required in a transaction, the smart card based personal ID card can protect the individual's privacy while ensuring the individual is properly identified.

**Strong Security**. When compared with other tamper-resistant tokens, smart cards currently represent the best compromise between security and cost. Smart cards allow backward compatibility with other installed card systems – co-existing with magnetic stripe, bar codes, embossing, or even simple visual printing on the same card. When used in combination with other technologies such as public key and biometrics, smart cards are almost impossible to duplicate or forge and data in the chip can't be modified without proper authorization (e.g., with passwords, biometric authentication or cryptographic access keys).

**Cost-Effective Offline Verification**. With small, secure, but low cost, portable readers, smart card based verification can be cost-effectively deployed at the various physical points that require validation of identity – for example, at different locations in an airport or other secure facility. Security officers can verify an individual's identity by comparing a scanned biometric with a biometric stored on the card, eliminating the need for online access to a central database.

**Online Electronic Signatures** (an application of digital identification). Many countries, including the U.S., are adopting laws (e.g., U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Electronic Signatures in Global and National Commerce Act of 2000) accepting digital signatures to facilitate online business and information exchange. Smart cards are seen as the most secure vehicle for implementing digital signatures in a public key infrastructure. Smart cards can securely store an owner's private and public keys and related certificates and are able to perform digital cryptographic operations, such as digital signatures, without ever releasing private keys outside of the chip.

**Information Storage Capacity**. While the memory capacity of the traditional magnetic stripe plastic card is quite limited, the memory capacity of a smart card is significant and can vary based on application. It is possible to have in the same system, if desired, low memory cards used for simple applications (e.g. an application to prove age) and higher memory cards used for more complex multiple applications. Today's smart card offers enough memory to store a compressed photo image, biometrics, digital certificates and public/private keys, as well as typical demographic alphanumeric files.

**Read and Write Capability**. Smart card technology protects information, but also allows updates in the field as long as the credentials of the requestor authorize the update. For example, an airline can update a traveler's profile during the security check process.

**Multiple Applications**. A smart card can host multiple applications to provide additional convenience and a more cost-effective implementation. The same smart card can be used to access protected web sites, to identify oneself to a specific authority, to secure online transactions, and to store a personal profile. In addition to online identification, that same card can provide access to state or city-based services such as social assistance, student and library services, or park and recreational programs. Each individual may have a different set of applications in the card depending on his/her lifestyle.

**Multiple Services**. Different organizations or service providers administering various services can use the same smart card. For example, the same card can be used by city authorities for secure physical and logical identification, by the city's Department of Education for student record and campus services, and by the social assistance agency for the administration of social assistance services.

As a result of its multi-application functionality and flexibility, a smart personal identification card can also play a key role in customizing services to a targeted population. For example, a program applying only to a certain segment of the population (such as a social assistance program) can be loaded to the identification cards for that population alone, rather than to all cards issued. In addition, the duration of such services can be customized per cardholder, enabling the card to verify eligibility without requiring card re-issuance.

**Contactless Capability**. Smart cards can also support the use of contactless technology, enabling applications that require rapid and secure identification, such as physical access to buildings and transportation services. By eliminating the need for physical card contact, contactless smart cards can be used to implement security processes with high throughput requirements (e.g., verifying traveler identity in high traffic transportation centers).

Smart card technology, coupled with an IT architecture and card management processes that are designed to protect the individual's identity information, provides a proven, cost-effective foundation for a secure personal identification system.

## Conclusion

Smart card based personal identification cards offer significant benefits for individuals, businesses and governments. Individuals using smart identification cards enjoy greater satisfaction through quicker and more secure access to information and services. The efficiency, consolidation of programs and security features provided through the use of smart identification cards enable governments and businesses to securely improve services, while reducing operating costs. And, through privacy-sensitive system designs, individual information can be protected from misuse.

Smart card based ID solutions are able to meet the requirements of a wide range of policy and legal mandates and provide the technical solution for secure identification. The Smart Card Alliance urges businesses and government officials to familiarize themselves with the enhanced functionality, operational and security advantages that smart card based personal IDs can provide to aid in the worldwide effort to improve identification processes and reduce identity fraud.

*For more information about smart cards and the role that they play in secure ID systems and other applications, please visit the Smart Card Alliance web site at www.smartcardalliance.org or contact the Smart Card Alliance directly at 212-571-0100.*

## About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, healthcare, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit www.smartcardalliance.org.

## Publication Acknowledgements

This white paper was developed by the Smart Card Alliance to discuss the implementation and technology issues associated with secure personal identification systems. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance. The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their comments and contributions.

Task force members include:

**Paul Beverly**, SchlumbergerSema
**Alan Bondzio**, ADB
**Kirk Brafford**, Xansa
**Thierry Burgess**, Oberthur
**John Burke**, Foley Hoag
**Peter Cerra**, Consultant
**Chris Corum**, AVISIAN Inc.
**Mike Dinning**, US Dept of Transportation
**Donna Farmer**, Smart Card Alliance
**Greg Garback**, WMATA
**Alex Giakoumis**, Atmel
**Kevin Gillick**, Datacard Group
**Bill Holcombe**, GSA
**Karen Jones**, IBM
**Mansour Karimzadeh**, ACI Worldwide
**Jeff Katz**, Atmel
**Diana Knox**, Visa
**Colleen Kulhanek**, Datakey
**Gilles Lisimaque**, Gemplus
**Cathy Medich**, Consultant
**Bob Merkert**, SCM Microsystems
**John Moore**, GSA
**Sandy Morris**, MasterCard
**Jim O'Connell**, Caradas
**Tate Preston**, Datacard
**Bill Randle**, Huntington
**Keith Saunders**, MasterCard
**Louis Sciupac**, LaserCard System
**Jennifer Spade**, CrossCom National
**Jeff Staples**, AVISIAN Inc.
**Guy Tallent**, Identrus
**Charles Walton**, Caradas
**Mike Weekes**, IBM
**Bob Wilberger**, Northrop Grumman IT
**Jody Zimmerman**, Consultant